Política de Segurança da Informação

Sumário

Introdução

Para proteger os recursos de tecnologia da informação da Pagare e proteger a confidencialidade dos dados, devem ser tomadas medidas de segurança adequadas. Esta Política de Segurança da Informação reflete o compromisso da Pagare de cumprir os padrões exigidos que regem a segurança de informações confidenciais e não confidenciais.

A Pagare pode minimizar exposições inadequadas de informações confidenciais ou sensíveis, perda de dados e uso inadequado de redes e sistemas de computadores, cumprindo padrões razoáveis (como o padrão de segurança de dados da indústria de cartões de pagamento), atendendo ao design e controle adequados dos sistemas de informação e aplicar sanções quando ocorrerem violações desta política de segurança.

A segurança é de responsabilidade de todos que usam os recursos de tecnologia da informação da Pagare. É de responsabilidade dos funcionários celetistas, prestadores de serviços e parceiros de negócios. Cada um deve se familiarizar com as disposições desta política e com a importância de segui-la ao usar os computadores, redes, dados e outros recursos de informação da Pagare.

Cada um é responsável por relatar qualquer violação suspeita de seus termos. Dessa forma, espera-se que todos os usuários de recursos de tecnologia da informação sigam todas as políticas e procedimentos exigidos pela Pagare.

Por fim, este documento apresenta um conjunto de instruções e procedimentos para normatizar e melhorar a visão e atuação em segurança da informação de forma a cumprir não apenas os regimentos interno, mas também normas, circulares e regulamentos do mercado de atuação da Pagare, entre elas estão: ISO 27001, Resolução Bacen 4658/18.

Objetivo

O objetivo principal desta política de segurança é estabelecer regras para garantir a proteção de informações confidenciais e garantir a proteção dos recursos de tecnologia da informação da Pagare. A política atribui responsabilidade e fornece diretrizes para proteger os sistemas e os dados da Pagare contra uso indevido ou perda.

Esta política de segurança se aplica a todos os usuários de sistemas de computadores, gerenciados centralmente ou computadores autorizados a se conectar à rede de dados da Pagare. Pode ser aplicado a usuários de serviços de informações operados ou administrados pela Pagare (dependendo do acesso a dados confidenciais etc.). Os indivíduos que trabalham para instituições afiliadas a Pagare estão sujeitos a essas mesmas definições e regras quando usam os recursos de tecnologia da informação da Pagare.

Esta política de segurança se aplica a todos os aspectos da segurança de recursos de tecnologia da informação, incluindo, entre outros, destruição acidental ou não autorizada, divulgação ou modificação de hardware, software, redes ou dados.

Esta política de segurança foi elaborada para abordar especificamente a segurança dos dados usados pelo setor de cartões de pagamento.

Os dados do cartão de crédito armazenados, processados ou transmitidos com o ID do comerciante devem ser protegidos e os controles de segurança devem estar em conformidade com o Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS).

Os dados do titular do cartão neste documento são definidos como Número da conta principal (PAN), Código de validação do cartão (CVC, CVV2 e CVC2), PIN do cartão de crédito e qualquer forma de dados de tarja magnética do cartão (Faixa 1, Faixa 2).

Responsáveis pela Política de Segurança

A Diretoria Operacional e Gerência de TI são os custodiantes atribuídos desta Política de Segurança. É da responsabilidade do custodiante (s) desta política de segurança para publicar e divulgar essas diretivas para todos os usuários relevantes da Pagare sistema (incluindo fornecedores, empreiteiros e parceiros de negócios).

Além disso, o (s) guardião (s) deve (m) garantir que a política de segurança endereça e esteja em conformidade com todos os padrões que a Pagare deve seguir (como o PCI DSS).

Este documento de política também será revisado pelo menos anualmente pelo (s) depositário (s) (e quaisquer proprietários de dados relevantes) e atualizado conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente de risco. Além de reportar aos órgãos competentes, quaisquer mudanças, a fim de mantê-los sempre atualizados.

Perguntas ou comentários sobre esta política devem ser direcionados ao (s) custodiante (s) listado (s) acima.

Documentos adicionais de processos e normas referenciadas por esta política

Este documento de política define as políticas de segurança da Pagare relacionadas à proteção de dados confidenciais e, principalmente, de dados de cartão de crédito. Detalhes sobre os padrões e procedimentos da Pagare em vigor para permitir que essas políticas sejam seguidas estão contidos em outros documentos referenciados por esta política.

A Tabela 2 lista outros documentos que acompanham este documento de política de segurança, que ajudam a definir as melhores práticas de segurança de dados da Pagare.

Documentos de processo e padrões de segurança

Nome do Documento	**Local/Departamento**
Procedimentos de retenção e armazenamento de dados	<Pagare/Pagare/TI/PoliticasSGSI> Departamento de TI
Processo de validação de conformidade do provedor de serviços	<Pagare/Pagare/TI/PoliticasSGSI> Departamento de TI
Plano de resposta a incidentes	<Pagare/Pagare/TI/PoliticasSGSI/Documentos> Departamento de TI

Parâmetros de segurança – padrão de senha

Os componentes do sistema usados em redes confidenciais geralmente vêm com as configurações padrão do fornecedor (nomes de usuário, senhas, configurações etc.). A política geral da Pagare é sempre alterar os padrões fornecidos pelo fornecedor para senhas do sistema e outros parâmetros de segurança antes que os sistemas sejam instalados no ambiente de rede seguro (rede de dados do titular do cartão).

Indivíduos com intenção maliciosa (externa e interna a uma entidade) geralmente usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bem conhecidas pelas comunidades de hackers e são facilmente determinadas por meio de informações públicas.

Serviço	Composição
Por domínio	As senhas têm um tempo de validade determinado pela equipe de segurança de 90 dias, devendo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas. As últimas 04 senhas não podem ser repetidas. Uma senha segura deve conter no mínimo 8 caracteres alfanuméricos (letras, maiúsculas e minúsculas e números/ símbolos).
BitBucket/Jira	As senhas sempre serão feitas e coordenadas pelo Administrador não podendo ser alterado pelo usuário. As senhas não têm validade. Uma senha segura deve conter no mínimo 8 caracteres alfanuméricos (letras, maiúsculas e minúsculas e números).
E-mail corporativo	É responsabilidade do Gerente de TI inserir e excluir um novo usuário e a senha deve ter 8 caracteres alfanuméricos (letras, maiúsculas e minúsculas e números).
GLPI	As senhas sempre serão feitas e coordenadas pelo Administrador não podendo ser alterado pelo usuário. As senhas não têm validade. Uma senha segura deve conter no mínimo 8 caracteres alfanuméricos (letras, maiúsculas e minúsculas e números).

A senha não deve ser jamais passada a ninguém, nem mesmo para a equipe de segurança. Caso desconfie que a senha não está mais segura, ela deve ser alterada, mesmo antes do prazo de validade.

Tudo que for executado com uma senha, será de inteira responsabilidade do seu detentor e está sujeito às sanções, por isso devem ser tomadas todas as precauções possíveis para manter a senha em caráter sigiloso e secreto.

Alterar padrões fornecidos pelo fornecedor

Todos os padrões fornecidos pelo fornecedor devem ser alterados em todos os componentes do sistema antes de serem utilizados na rede de dados do titular do cartão. (por exemplo, senhas, cadeias de comunidades SNMP (protocolo de gerenciamento de rede simples) e eliminação de contas desnecessárias etc.). (Requisito 2.1.a, 2.2.d do PCI DSS)

Todas as contas padrão desnecessárias devem ser removidas ou desativadas antes de instalar o dispositivo na rede. (Requisito 2.1.b do PCI DSS)

Desenvolver e Manter Sistemas e Aplicativos Seguros

Indivíduos sem escrúpulos usam vulnerabilidades de segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são corrigidas por patches de segurança fornecidos pelo fornecedor, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os sistemas devem ter todos os patches de software apropriados para proteger contra a exploração e o comprometimento dos dados do titular do cartão por indivíduos e softwares maliciosos.

Nota: Os patches de software apropriados são aqueles que foram avaliados e testados o suficiente para determinar que os patches não entram em conflito com as configurações de segurança existentes.

Para aplicativos desenvolvidos internamente, inúmeras vulnerabilidades podem ser evitadas usando processos de desenvolvimento de sistema padrão e técnicas de codificação seguras.

Atualizar regularmente sistemas e software

Todos os componentes e software do sistema devem ter os patches de segurança mais recentes fornecidos pelo fornecedor instalados. (Requisito 6.2.a do PCI DSS).

Todos os patches críticos de sistema e software devem ser instalados dentro de 30 dias após a liberação do fornecedor. (Requisito 6.2.b do PCI DSS).

Identificação e Autenticação de acesso

É fundamental atribuir uma identificação exclusiva (ID) a cada pessoa com acesso a sistemas ou software críticos. Isso garante que cada indivíduo seja o único responsável por suas ações. Quando essa responsabilidade está em vigor, as ações executadas em dados e sistemas críticos são executadas e podem ser rastreadas para usuários conhecidos e autorizados.

Exigir Ids de usuário exclusivo

IDs exclusivos serão usados para todos os usuários que acessam os componentes do sistema no ambiente de dados do titular do cartão. (Requisito 8.1 do PCI DSS)

Revogar imediatamente o acesso de qualquer usuário encerrado. (Requisito 8.1.3 do PCI DSS)

Métodos de autenticação do usuário

Além de atribuir um ID de usuário exclusivo, o acesso aos sistemas na rede exige o uso de pelo menos um dos seguintes itens: (Requisito 8.2 do PCI DSS)

- Algo que você sabe, como uma senha ou frase secreta.
- Algo que você tem, como um dispositivo token ou cartão inteligente.
- Algo que você é, como um biométrico.

As senhas ou frases devem atender ao seguinte: (Requisito 8.2.3 do PCI DSS)

- Exigir um comprimento mínimo de pelo menos sete caracteres.
- Contêm caracteres numéricos e alfabéticos.

Contas e senhas em grupo ou compartilhadas

Não use contas ou senhas de grupo, compartilhadas ou genéricas ou outros métodos de autenticação, como a seguir: (Requisito 8.5 do PCI DSS.).

- IDs de usuário genéricos estão desativados ou removidos.
- IDs de usuário compartilhados não existem para administração do sistema e outras funções críticas.
- IDs de usuário compartilhados e genéricos não são usados para administrar nenhum componente do sistema.

Liberação de Acessos

Responsável pela Liberação de pastas na Rede Interna	
Diretoria/Administrativo/Comercial/RH/ Financeiro/Marketing/Parceiros	Gerente de Negócios
Fábrica	Gerente de Projeto
Suporte	Gerente de TI
TI	Gerente de TI
Público	Uso Livre

Responsável pelo Acesso aos Servidores e Aplicações	
GLPI	Gerente de TI
Trac/SVN/BitBucket	Gerente de Projeto
Banco de Dados	Gerente de Projeto
RPNet	Gerente de Projeto
Servidores	Gerente de Projeto/Gerente de TI
Serviços Cloud	Gerente de Projeto/Gerente de TI

Os acessos e senhas não deve ser jamais passada a ninguém, nem mesmo para a equipe de segurança. Caso desconfie que a senha não está mais segura, ela deve ser alterada, mesmo antes do prazo de validade.

Tudo que for executado com uma senha, será de inteira responsabilidade do seu detentor e está sujeito às sanções, por isso devem ser tomadas todas as precauções possíveis para manter a senha em caráter sigiloso e secreto.

Acesso para Colaboradores

Toda vez que um novo colaborador entrar na Pagare, o Gestor Responsável enviará um e-mail para o suporte Pagare informando a necessidade de criação de um usuário e os acessos que ele deverá ter.

A área de suporte abrirá um ticket no sistema de chamados GLPI.

No caso de uma necessidade de mudança, quer seja por integração a um novo projeto, mudança de função ou cargo, caberá ao gestor novamente fazer o mesmo processo.

Caberá a área de TI fazer avaliações periódicas desses acessos junto aos gestores e manter atualizado em sua Planilha de Controle e Mapeamento de Rede. Essa avaliação não deve ser superior a seis meses.

Qualquer exceção de acesso deve ser autorizada pelo gestor imediato justificando no chamado e é cabível de análise e aprovação da área de segurança da informação.

O usuário deve ter todo cuidado ao ter acesso a pasta/servidor, pois todos os acessos terão privilégios de exclusão, inclusão e revisão de dados.

Acesso de Visitantes

Cabe ao responsável pelo visitante solicitar acesso também pelo e-mail do suporte Pagare, nesse caso informando o período de início e término da atividade e tipo de acesso necessário, quando seus trabalhos forem temporários.

Caso haja necessidade de extensão do tempo caberá ao gestor da área fazer um novo e-mail.

A área de suporte abrirá um ticket no sistema de chamados GLPI e entregará para o visitante o Termo de Confidencialidade para que seja assinado.

Desligamento de Colaborador

Para desligamentos de colaborador caberá ao Gestor Responsável enviar um e-mail para o suporte Pagare informando a saída do mesmo e a data que devem ser retirados todos os acessos.

Para equipamentos verificar item Equipamentos desta política.

Restrição de Acesso aos Dados do Titular do Cartão

Qualquer acesso físico a dados ou sistemas que abrigam os dados do titular do cartão oferece a oportunidade para os indivíduos acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, devendo ser adequadamente restrito.

Nota: Para os fins do Requisito "pessoal no local" refere-se a funcionários de tempo integral e meio período, funcionários temporários, contratados e consultores que estão fisicamente presentes nas instalações da entidade. Um "visitante" refere-se a um fornecedor, convidado de qualquer equipe no local, técnicos de serviço ou qualquer pessoa que precise entrar na instalação por um curto período, geralmente não mais que um dia. “Mídia” refere-se a toda mídia em papel e eletrônica que contém dados do titular do cartão.

Proteção de Mídias

A Pagare definirá procedimentos específicos para proteger fisicamente todas as mídias, incluindo, entre outros, computadores, mídia eletrônica removível, recibos em papel, relatórios em papel. (Requisito 9.5 do PCI DSS).

Distribuição de mídia

Mantenha controle rígido sobre a distribuição interna ou externa de qualquer tipo de mídia, incluindo o seguinte: (Requisito 9.6 do PCI DSS).

- Classifique a mídia para que a sensibilidade dos dados possa ser determinada.
- Envie a mídia por correio expresso ou outro método de entrega que possa ser rastreado com precisão. Os logs devem mostrar aprovação da gerência e informações de rastreamento. Reter logs de transferência de mídia.
- Verifique se o gerenciamento aprova todas as mídias que são movidas de uma área segura, inclusive quando a mídia é distribuída a indivíduos.

Armazenamento e acessibilidade

Manter o controle rígido sobre o armazenamento e acessibilidade da mídia. (Requisito 9.7 do PCI DSS).

Manter adequadamente os registros de inventário de todas as mídias e realizar inventários de mídia pelo menos anualmente. (Requisito 9.7 do PCI DSS).

Políticas e procedimento de destruição de mídia

A mídia que contém dados do titular do cartão deve ser destruída quando não for mais necessária por motivos comerciais ou legais. (Requisito 9.8 do PCI DSS).

A Pagare deve definir e documentar procedimentos específicos que serão usados para destruir, além da reconstrução, qualquer material impresso que contenha os dados do titular do cartão. Tecnologias como trituração, incineração, polpação etc. devem ser usadas para destruir a mídia. (Requisito 9.8.1 do PCI DSS).

Se aplicável, todos os contêineres usados para armazenar mídia contendo os dados do titular do cartão a serem destruídos devem estar sempre trancados e em uma área segura. Esses recipientes devem ser entregues apenas a pessoal autorizado ou a terceiros para fins de destruição. (Requisito 9.8.1.b do PCI DSS).

Diretiva de Segurança da Informação

Informação é todo conjunto de dados que tenha sido tratado, agrupado, transformado e/ou consolidado, possuindo valor para a empresa, seu negócio, seus produtos e ou para seus colaboradores, parceiros de negócio, fornecedores e clientes.

A informação pode se encontrar em várias mídias de transmissão e armazenamento, podendo ser impressa e ou armazenada em meios magnéticos e óticos

Sem políticas e procedimentos de segurança fortes, muitas das camadas de controles de segurança se tornam ineficazes para impedir a violação de dados.

A menos que políticas e práticas consistentes sejam adotadas e seguidas o tempo todo, os controles de segurança quebram devido à falta de atenção e manutenção deficiente.

Por fim, o não cumprimento dessas políticas acarretará sanções administrativas em primeira instância, podendo ocorrer desligamento do funcionário de acordo com a

gravidade da ocorrência e rescisão de contratos com os terceiros prestadores de serviços.

Gestão da Informação

Toda informação produzida deve ter um proprietário.

O proprietário da informação será sempre o executivo ao qual a unidade de negócio produtora da informação está subordinada. O proprietário da informação poderá delegar a gestão da informação a um colaborador da unidade de negócio produtora da informação, que poderá administrar as divulgações e liberação de acessos.

Guarda da Informação

Todos os documentos devem ser armazenados no servidor corporativo, evitando salvar no disco local das estações de trabalho.

Os documentos controlados e acessíveis a todos os colaboradores deverão estar disponíveis. Contudo, sem condições de exclusão, inclusão ou revisão dos documentos.

Em relação ao tempo de guarda dos documentos, deverá ser observado o tempo exigido pela legislação em vigor para cada caso e na Matriz de Registros e Matriz de Documentos.

Classificação da Informação

O gestor da informação, proprietário da informação ou seu delegado.

Os documentos (políticas e procedimentos) e modelos de formulários encontram-se no SharePoint.

Informações Confidenciais só podem ser divulgadas pelo proprietário da informação, devendo selecionar os colaboradores que irão receber as mesmas.

- Informações Restrito podem ser divulgadas ou ter seu acesso liberado pelo gestor da informação conforme a necessidade do negócio. A formalização da liberação de acesso requer aprovação do proprietário da informação.
- Informações Públicas podem ser divulgadas ou ter seu acesso liberado livremente a todos os colaboradores da empresa.

A divulgação ao público externo de qualquer informação requer aprovação prévia do proprietário da informação.

Tabela de Classificação da Informação

Para visualização do tipo de documentação e forma de controle, deve ser visto na Política de Gestão de Documentos e Registros.

Contratos com Partes Externas

Todos os documentos externos (incluindo contrato) devem ser armazenados no servidor corporativo, evitando salvar no disco local das estações de trabalho.

Na pasta de documentos externos deverá ter uma subpasta inserida o contrato atual e documentos extras no qual devem ser considerados para compor evidência da segurança necessária.

Segurança Física e do Ambiente

Controle de Acesso à área Restrita

A sala deve sempre permanecer trancada. O acesso à mesma só poderá ser feito para área de TI (suporte, segurança, rede e desenvolvimento) e demais colaboradores e visitantes só poderão entrar mediante aprovação prévia do Gerente de Projeto ou Gerente de TI informando no Controle de Acesso (nome, RG, empresa, horário de entrada e saída e motivo).

Controle de Acesso a Demais Áreas

O acesso é livre a demais áreas a todos os colaboradores envolvidos.

Para visitantes caberá ao mesmo a se dirigir a recepção para acesso.

Notificação de Fragilidades

Qualquer fragilidade e eventos indesejáveis de segurança devem ser comunicados imediatamente para área de Suporte (por e-mail ou telefone). A área deverá abrir um chamado, avaliar o ocorrido e realizar as ações necessárias.

Caso necessário e aplicável, ações de contingência devem ser dadas (de acordo com definição na Política Risco e Contingência) e avaliar posteriormente as causas do

problema e possíveis ações de mudanças (Ver Política de Gestão de Melhoria Contínua e Política de Gestão de Mudança).

Internet

A internet deve ser utilizada, de acordo com o Termo de Uso e Política de Uso da Internet e exclusivamente, para fins corporativos. O uso pessoal deve ser moderado e de forma breve.

A empresa pode, sem aviso prévio, restringir o acesso a qualquer site que apresente conteúdo impróprio, ou que não esteja relacionado aos seus interesses, como por exemplo:

- Pornográfico ou pedófilo;
- Apologia a racismo e/ou terrorismo;
- Apologia ao crime ou a drogas;
- Download de programas ou arquivos fora dos interesses da empresa;
- Hackers;
- Salas de bate-papo fora dos interesses da empresa, incluindo programas de comunicação instantânea e redes sociais, por exemplo, Facebook, Instagram, Twitter, WhatsApp etc.;
- Comércio eletrônico fora dos interesses da empresa;
- Jogos, incluindo jogos de azar;
- Download de vídeos, jogos etc.

A utilização da internet é constantemente monitorada, sendo este monitoramento realizado de forma geral. Os casos de tentativa de acesso aos sites que não sejam de interesse da empresa ou a realização de downloads proibidos, são levados ao gestor imediato.

E-mail

Não devem ser abertos anexos de e-mail com as extensões:

• .bat,

• .exe,

- .src,
- .lnk
- .com
- .sh
- .bin
- .dll

E-mails com assuntos estranhos e/ou em inglês são objetos de desconfiança.

Evite anexos muito grandes. A capacidade máxima de envio será de 20MB.

Estação de Trabalho

Cada estação de trabalho possui um nome que permite identificá-la na rede.

Cada profissional é responsável pelo seu perfil e se ele tiver perfil de administrador também será responsável pela estação de trabalho em uso.

Os colaboradores estarão sujeitos às sanções de que trata o item 2. Por isso sempre que sair da estação, tenha certeza de que o logoff ou bloqueio da tela (com senha) foi efetuado.

- Para Windows: Janela + Letra “L”;
- Para Linux: Crtl + Alt + “L”;
- Para Mac: Comand + Shift + “Q”;
- Não instale nenhum tipo de software/hardware sem autorização da área de TI;
- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria gravada no equipamento;
- Não deixe informações da empresa gravadas na estação de trabalho que possam prejudicar o backup.

O uso de removíveis não é recomendado aos colaboradores. Os administradores de rede devem avaliar a criticidade do uso para as áreas na Planilha de Risco e Planilha de Controle Mapeamento de Rede.

Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup.

Backup e Restore

A estrutura de backup e restore está definido conforme tabela abaixo:

RPNet	Realizado pela GCP e Azure e controlado através do SLA assim como restauração
Rede/SNV/TRAC/BitBucket	Será feito backup todos os dias incremental e uma vez por mês completo no servidor e um hd externo. O hd externo deverá ser trocado mensalmente e o anterior arquivado fora da empresa com Gerente de TI. Restauração a ser feita de acordo com a necessidade e pedido do solicitante.
E-mail	Será feito pelo fornecedor de e-mail e fica disponível enquanto em uso. A recuperação é automática a partir da aplicação GoogleVault
GLPI	Processo feito diariamente e enviado para rede. O backup será feito de acordo definido na rede.

Vírus e Código Malicioso

Mantenha o antivírus atualizado e caso perceba que a atualização não está funcionando, entre em contato com a área de TI para que a situação possa ser corrigida.

Não traga CDs PenDrives, HD externos ou quaisquer outros dispositivos de armazenamento de dados para dentro da empresa.

Reporte atitudes suspeitas no sistema para área de TI, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

Todo dia ao meio-dia, o antivírus efetuará uma varredura para avaliação. Todos os colaboradores deverão deixar suas máquinas ligadas para que a operação seja feita adequadamente.

Os relatórios gerados serão avaliados pela equipe de TI semanalmente.

Para uso de removíveis, o antivírus está instalado para avaliar o dispositivo ao ser conectado na rede.

Sistemas

Os sistemas da Pagare devem ser utilizados única e exclusivamente para as finalidades da empresa, não podendo adulterar ou utilizar qualquer informação em benefício próprio.

Nenhum colaborador poderá instalar ou desinstalar um software. Esta é uma atribuição de responsabilidade exclusiva do suporte.

Em caso de necessidade de compra de um novo software, caberá ao Gestor encaminhar um e-mail para a área de suporte, sendo que este deverá abrir um ticket no GLPI e encaminhar para área financeira para aprovação.

Após a aprovação, a área de TI efetua a aquisição e quando da sua chegada deverá conferir as informações e inserir o software na Planilha de Ativos.

Equipamentos

Utilizar somente softwares e equipamentos autorizados, homologados e de propriedade da Pagare, zelando e guardando-os em local seguro.

A responsabilidade é do colaborador devendo este assinar o Termo de Responsabilidade. Para esse item caberá que o Gerente de TI informe no formulário quais recursos e equipamentos estão disponibilizados para o colaborador.

Comunicar imediatamente à área de TI quaisquer irregularidades ou problemas com o equipamento.

Devolver o equipamento no caso de rescisão de contrato de trabalho ou substituição de equipamento e assinar o Termo de Devolução como comprovante da entrega e das condições adequada do equipamento.

Controle de Ativos

Cabe à área de TI atualizar a Planilha de Ativos sempre que um novo hardware, software, equipamentos de telecomunicações forem inseridos, alterados ou removidos.

Ativos a serem controlados

- ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- ativos físicos: equipamentos computacionais (processadores, monitores, laptops, modems), equipamentos de comunicação (roteadores, PABXs), mídia magnética (fitas e discos), outros equipamentos técnicos (nobreaks, ar-condicionado).

As informações mais detalhadas estão especificadas na Política de Ativos.

Gestão Segura de Identidade

Gerencia identidades de pessoas que acessam os recursos da empresa e "habilita os indivíduos corretos a acessar os recursos corretos no momento correto e pelos motivos corretos". Essa prática garante à Pagare que somente terão acesso em sua plataforma os dispositivos autorizados a realizar transações por meio dela.

- Para API (Application Programming Interface ou Interface de Programação de Aplicações) o cliente recebe uma chave de acesso e certificados de segurança SSL/TSL.
- Para APP (Aplicativo Móbile ou Aplicativo Móvel) o cliente recebe um login de acesso no app da conta digital.

Manter Política de Segurança da Informação para Todos

Uma política de segurança forte define o tom de segurança para Pagare e informa os funcionários e fornecedores o que é esperado deles. Todos os funcionários e fornecedores devem estar cientes da sensibilidade dos dados e de suas responsabilidades em protegê-los.

Nota: "Funcionários" refere-se a funcionários de tempo integral e meio período, funcionários e funcionários temporários e contratados e consultores "residentes" no site da empresa.

Resultados em uma avaliação formal de riscos (Requisito 12.2 do PCI DSS)

Política de compartilhamento de dados com provedores de serviços

Para estar em conformidade com as melhores práticas do setor, é necessário que a devida diligência seja realizada antes de se envolver com novos provedores de serviços e seja monitorada pelos provedores de serviços atuais que armazenam, processam ou transmitem dados do titular do cartão em nome da Pagare. Os provedores de serviços, que podem afetar a segurança dos dados confidenciais do titular do cartão, também estão no escopo desta política.

A Pagare deve manter uma lista documentada de todos os provedores de serviços aplicáveis em uso. (Requisito 12.8.1 do PCI DSS)

É necessário um contrato por escrito com todos os provedores de serviços aplicáveis e deve incluir um reconhecimento da responsabilidade dos provedores de serviços de proteger todos os dados do titular do cartão que recebem de ou em nome da Pagare ou na medida em que possam afetar a segurança de um ambiente de dados do titular do cartão (requisito 12.8.2 do PCI DSS). Além disso, o provedor de serviços deve concordar em fornecer evidências de validação de conformidade anualmente. (Requisito 12.8.4 do PCI DSS). Antes de se envolver com um provedor de serviços aplicável, deve-se seguir um processo completo de due diligence. (Requisito 12.8.3 do PCI DSS)

A Pagare deve revisar anualmente as evidências fornecidas pelos provedores de serviços aplicáveis, demonstrando sua conformidade contínua com o PCI DSS. (Requisito 12.8.4 do PCI DSS)

A Pagare deve manter uma lista de quais requisitos do PCI DSS são gerenciados por cada provedor de serviços e que são gerenciados por Phoebus, Adiq, PagSeguro e Pax. (Requisito 12.8.5 do PCI DSS)

Plano de resposta a incidentes

Incidentes ou suspeitos relacionados à segurança da rede de dados do titular do cartão ou dos próprios dados do titular do cartão devem ser tratados rapidamente e de

maneira controlada, coordenada e específica. Um plano de resposta a incidentes (IRP) deve ser desenvolvido e seguido no caso de uma violação ou suspeita de violação. As políticas a seguir abordam especificamente o IRP da Pagare.

A Pagare deve manter um IRP documentado e estar preparado para responder imediatamente a uma violação do sistema. (Requisito 12.10 do PCI DSS)

Apêndices

Apêndice A – Funções e responsabilidades de gerenciamento

Conforme exigido pela política na Seção 12.5 desta política de segurança, a tabela a seguir contém a atribuição de funções de gerenciamento para processos de segurança.

Função/Departamento	Data	Descrição
Gerencia de TI	08/11/2022	Estabelecer, documentar e distribuir políticas de segurança
Gerencia de TI	08/11/2022	Monitorar, analisar e distribuir alertas e informações de segurança
Gerencia de TI	08/11/2022	Estabelecer, documentar e distribuir políticas de resposta e escalação de incidentes de segurança
Gerencia de TI	08/11/2022	Administração de contas de usuário em sistemas na rede de dados do titular do cartão
Gerencia de TI	08/11/2022	Monitorar e controlar todo o acesso aos dados do titular do cartão

Apêndice B – Acordo de cumprimento

Todos os funcionários que trabalham com dados do titular do cartão devem enviar uma cópia impressa assinada deste formulário. A gerência da Pagare não aceitará modificações nos termos e condições deste contrato.

_____

Nome impresso do funcionário

_____

Departamento de funcionários

_____
Número de telefone do funcionário

_____
Endereço físico e localização do correio do funcionário

Eu, _____, concordo em tomar todas as precauções razoáveis para garantir que as informações internas da Pagare ou as informações confiadas ao Pagare por terceiros, como clientes, não sejam divulgadas a pessoas não autorizadas. No final do meu emprego ou contrato com a Pagare, concordo em retornar a Pagare todas as informações às quais tive acesso como resultado de minha posição com a Pagare. Entendo que não estou autorizado a usar essas informações para meus próprios fins, nem tenho a liberdade de fornecer essas informações a terceiros sem o consentimento expresso por escrito do gerente interno de Pagare que é o proprietário designado das informações.

Tenho acesso a uma cópia do Manual de diretivas de segurança da informação Pagare, li e compreendi o manual e entendo como isso afeta meu trabalho. Como condição de emprego contínuo na Pagare, concordo em cumprir as políticas e outros requisitos encontrados nesse manual. Entendo que o não cumprimento será motivo de ação disciplinar, incluindo revogação de privilégios do sistema, demissão de Pagare e talvez penalidades criminais e/ou civis.

Concordo em escolher uma senha difícil de adivinhar, conforme descrito no Manual de Políticas de Segurança da Informação Pagare, concordo em não a compartilhar com nenhuma outra pessoa e concordo em não anotar essa senha, a menos que tenha sido transformada em uma maneira irreconhecível.

Também concordo em relatar imediatamente todas as violações ou suspeitas de violações das políticas de segurança da informação a Gerência de TI.

_____
Assinatura do funcionário

Histórico de Versionamento

Autor	Motivo	Data	Versão
Danilo de Souza	Versão Inicial	05/09/2013	1.0
Flavio Espuri	Revisão	22/10/2014	2.0
Daisy Leite	Revisão	01/09/2018	3.0
Cesar Martins	Revisão	07/12/2018	3.1
Carla do Carmo Cruz	Revisão	09/10/2020	3.2
Fernando P. Candido	Revisão	26/04/2021	3.3
Regiane Cruz	Complementação e alteração do Layout	22/09/2023	3.4

Aprovação da Política

Aprovador	Data
Gerente de Negócios	08/11/2022
Gerente de Projeto	08/11/2022
Gerente Administrativo e Comercial	08/11/2022
Gerente de TI	08/11/2022